

TI - Digital communication method for enciphering device - transmitting using special pattern, checking synchronisation with super frame signal and changing key code after communication partner has received signals

AB - J06237248 The digital communication method involves transmission of a signal from a transmitter including a special pattern. The signal for synchronisation (2) is received after frame synchronisation at the receiver. The frame transmission starts with a super frame signal (3) and a check synchronisation (MQ) is performed with the help of a key code.

- The key change timing is transmitted in the super frame signal for locating the frame position. After the communication partner has received the signal, the key code changes from the previously specified code.

- ADVANTAGE - Reliable operation. Enables timing change without interrupting communication.

- (Dwg.3/3)

PN - JP6237248 A 19940823 DW199506 H04L9/06 005pp

PR - JP19930022751 19930210

PA - (NITE) NTT IDO TSUSHINMO KK

MC - W01-A05A W01-A06C4

DC - W01

IC - H04B7/26 ;H04L9/06 ;H04L9/14

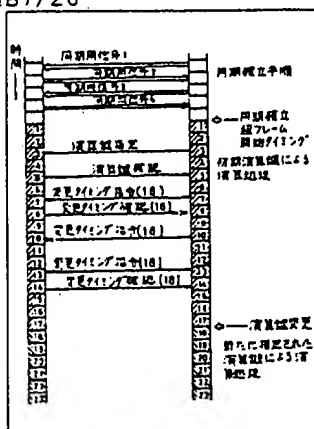
AN - 1995-039951 [06]

```

TI - DIGITAL COMMUNICATION METHOD
AB - PURPOSE:To change a cipher key during communication without interrupting
    the communication.
    - CONSTITUTION:A synchronizing signal including a special pattern is
      transmitted from the transmission side, and a synchronizing signal 2
      indicating that frame synchronism is established is received from the
      reception side, and the number of frames from the current frame to the
      start of a superframe is transmitted by a synchronizing signal 3, and a
      synchronizing signal 4 for confirmation which indicates the reception of
      this signal 3 is received. Thereafter, a cipher key is designated and
      transmitted, and its reception is confirmed, and a key change timing is
      transmitted as a preceding frame position in the superframe, and its
      reception is confirmed, and the cipher is switched to another cipher
      based on this designated cipher key at this change timing.

PN - JP6237248 A 19940823
PD - 1994-08-23
ABD - 19941128
ABV - 018623
AP - JP19930022751 19930210
GR - E1635
PA - N T T IDOU TSUUSHINMOU KK
IN - ONOE SEIZO; others: 03
I - H04L9/06 ;H04L9/14 ;H04B7/26

```



This Page Blank (uspto)

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平6-237248

(43)公開日 平成6年(1994)8月23日

(51)Int.Cl. ⁴	識別記号	庁内整理番号	FI	技術表示箇所
H 0 4 L 9/06				
H 0 4 B 7/26	1 0 9 N	7304-5K		
		7117-5K	H 0 4 L 9/02	Z

審査請求 未請求 請求項の数 1 O L (全 5 頁)

(21)出願番号 特願平5-22751

(22)出願日 平成5年(1993)2月10日

(71)出願人 392026693

エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番1号

(72)発明者 尾上 誠蔵

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(72)発明者 前原 昭宏

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(72)発明者 大戸 豊

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(74)代理人 弁理士 草野 卓 (外1名)

最終頁に続く

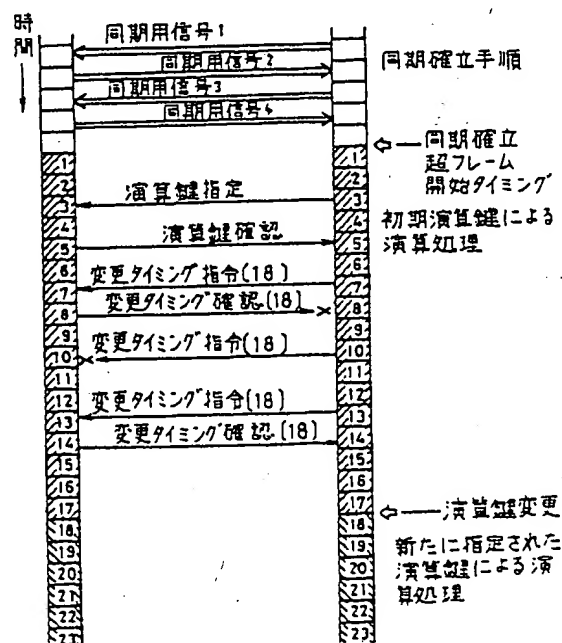
(54)【発明の名称】 デジタル通信方法

(57)【要約】

【目的】 通信中の暗号鍵の変更を、通信を中断することなく行う。

【構成】 送信側から特殊ボタンを含む同期用信号を送信し、受信側からフレーム同期が確立したことを示す同期用信号2を受信し、現フレームから超フレームの開始までのフレーム数を同期用信号3で送信し、これを受信したことを示す確認の同期用信号4を受信し、その後、暗号鍵を指定して送信し、その受信を確認後、鍵変更タイミングを、超フレーム内の先行するフレーム位置として送信し、これを受信したことを確認後、先の変更タイミングで先に指定した暗号鍵による暗号に切替える。

図 3



【特許請求の範囲】

【請求項1】 送信側で通信相手と周期の同期を確立し、当該周期内の時間的位置に対応した演算を情報に施して送信し、受信側で上記周期内の同一時間的位置で上記演算の逆演算を受信信号に施して元の情報を得るデジタル通信方法において、

上記演算の方法を変更するタイミングに関する情報を上記周期内の先行する時間的位置情報として上記通信相手に送信し、

上記タイミングに関する情報を上記通信相手が受信したことを確認した後、

上記タイミングに関する情報に基づいたタイミングで上記演算の方法を変更するデジタル通信方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、デジタル信号に暗号化等の演算処理を行って伝送し、しかもその演算の方法、つまり暗号化方法や暗号化の鍵を通信途中で変更するようにしたデジタル通信方法に関するものである。

【0002】

【従来の技術】例えば移動通信方式として一定周期のフレームを構成し、そのフレーム内のビット配置により通信チャネル情報と制御チャネル情報とを多重化して伝送する無線デジタル通信方式があり、その通信チャネル情報と制御チャネル情報との両者の情報内容を暗号化して伝送することがあるが、その際に、複数のフレームで超フレームを構成し、その超フレーム同期タイミングを暗号化処理の同期に用いる。この超フレーム周期を極めて長くし、かつ、通信を開始する際のフレーム同期手順でタイミングに関する情報をやりとりして、超フレームの開始タイミングの同期を同時に確立する方法がある。

【0003】この方法を採用して前記例では共通制御チャネルを利用して移動局が基地局と制御信号のやりとりを行って無線周波数の割り当てを受け、同期を確立し、通信中になった後に、つまり加入者番号（それまで移動局番号）による通信に入るが、同一の移動局を複数の加入者が利用するため、通信の安全性の点から、暗号化の鍵を変更する場合、両通信ノードでの鍵の変更が食い違くと通信中の制御チャネル情報による制御信号のやりとりも不可能になり、通信はもとより制御不能状態に陥る。

【0004】従ってこのように通信中に確実に鍵を変更するためには、通信中の制御チャネル情報を利用して次に使用する鍵を指定し、その後、無線チャネルの再割当てを要求、つまり、通信中チャネル切替えを要求し、この通信中チャネル切替えの手順をふんで同期を確立し、その際に新たな鍵を用いることが考えられる。

【0005】

【発明が解決しようとする課題】このように通信中チャネル切替え手順で同期を確立すると同時に暗号化の鍵を

変更する方法を採用した場合、暗号化の鍵を変更する際に、一時的に同期がはずれ再度同期が確立するまでの間、通信が中断するという欠点が生じる。この発明の目的は、通信中に暗号化等の演算処理方法を変更する際に通信が中断することのないデジタル通信方法を提供することにある。

【0006】

【課題を解決するための手段】通常、暗号化のような演算処理は、通信相手と周期の同期を確立し、その周期内の時間的位置に対応した演算を情報に施して送信し、受信側では上記周期内の同一時間的位置に上記演算の逆演算を受信信号に行って元の情報を得るが、この発明では演算方法を変更するタイミング情報を上記周期内の先行する時間的位置情報として通信相手に送信し、そのタイミングに関する情報を通信相手が受信したことを確認した後、上記タイミングに関する情報に基づいたタイミングで演算方法の変更を行う。

【0007】

【実施例】送信側において通信チャネル情報と制御チャネル情報が符号化回路1に入力される。符号化回路1では、その入力された通信チャネル情報と制御チャネル情報を、タイムベース2で定められた一定の長さ毎に区切り、多重化し、誤り訂正符号化、フレーム同期信号付与等を行う。その符号化回路1の出力は演算回路3で情報ビットに対して演算鍵設定回路4からの演算鍵に応じた予め定められた演算処理を行う。この演算鍵は制御回路5から指定設定される。演算回路3の演算処理は、一般には毎フレーム同一の演算ではなく、フレーム毎に異なる。即ち、タイムベース2からのフレームタイミングを計数するカウンタ6から入力されるフレーム数により時間経過を認識し、そのフレーム数に応じた演算処理を行う。例えば、この演算は暗号化処理であり、非常に長い周期の超フレーム内のフレーム位置で処理が定まる。演算回路3の出力は、送信回路7により、無線信号に変換されて送信される。

【0008】受信側は、送信側と超フレームの同期を最初に確立してあり、受信回路8で受信された信号はフレーム検出回路9に入力され、フレーム同期信号の検出等によりフレームタイミングが検出される。一方、受信された信号は演算回路10にも入力され、演算鍵設定回路11からの演算鍵に応じた演算処理が施される。演算鍵設定回路11は制御回路12から演算鍵が指定設定される。この演算鍵は、予め送信側との制御信号の授受により同じ演算鍵を設定し、演算処理は、送信側の処理の逆演算処理を行う。しかも超フレーム中の同一フレームに対して送信側の演算と逆の演算を行うため、カウンタ13によりフレーム検出回路9で検出したフレームのタイミングを計数し、その計数したフレーム数を演算回路10及び制御回路12へ供給する。これにより、送信側の元の情報に復元された情報が演算回路10から得られ、

この情報は符号回路14により、誤り訂正符号の復号処理や通信チャネル情報と制御チャネル情報との分離が行われる。図には示していないが実際には双方向通信に適用され、図中の送信側に受信側と同様の構成がまた受信側に送信側と同様の構成が設けられ、逆方向の通信についても、全く同様の処理が行われ、制御チャネル情報の双方向通信が行われる。

【0009】図2に、フレーム信号の構成例を示す。特定のビットパターンであるフレーム同期信号でフレーム位置を認識できるようにし、そのフレーム同期信号からの定められた相対位置に制御チャネル情報と通信チャネル情報を配置することにより多重化する。一般に通信チャネル情報は、通話している音声をデジタル符号化したものや、データサービス用の情報であり、制御チャネル情報は、無線通信のための周波数の再指定等、通信回線を維持するために必要な制御のための情報である。

【0010】図3はこの発明の実施例における通信中の演算鍵の変更手順を示す。通信を開始するために、通信用の無線チャネルを設定する際に、ある特定パタンの同期用信号を授受して、ビット同期やフレーム同期を確立する。この同期用信号の中に超フレームに関する情報を含めて送受し、超フレームの同期を同時に確立する。これは、例えば、同期用信号1で特定パタンの同期用信号を送り、これと同期し、つまりフレーム同期した確認を同期用信号2で受信し、同期用信号3で現フレームから超フレームの開始位置までのフレーム数を送り、同期用信号4で同期用信号3の受信フレーム位置から算出される超フレームの開始位置までのフレーム数を送り、受信側で超フレームの同期が確立したことを確認してから、同期用信号を授受する状態から通常の通信状態に移することにより実現できる。一般には同期用信号の受信を受信失敗する場合があります、同じ同期用信号3や同期用信号4を連続送信することにより対処するが、超フレームの開始位置までのフレーム数は、送信フレーム毎にカウントダウンした値を送る。同期用信号3や同期用信号4などは制御チャネル情報に対して演算鍵による演算がなされた状態で授受される。

【0011】以上のように同期が確立して通信状態に移移すると、通信状態に入る前に設定された演算鍵に基づいた演算、及び逆演算を図1中の演算回路3、10で実施する。演算鍵の変更在先立ち、制御チャネル情報で一方から新しい演算鍵を送り、相手からのその受信確認を受信する。その制御チャネル情報による送受はそれまでの演算鍵で演算処理して行く。なおこの新しい演算鍵の指定(送信)においては、直接演算鍵を転送するのではなく、ある値を転送し、両通信ノードに予め設定した秘密鍵と転送されたある値との定められた演算結果を演算鍵としてもよい。

【0012】次に、一方から演算処理の変更タイミングを示す情報を送信し、その確認を受信してからその変更

タイミングを示す情報に基づくタイミングで演算鍵を変更した演算に切り替える。変更タイミングを示す情報として、変更するフレームの超フレーム内の先行する(現フレームより先の)フレーム位置を表す値で示せばよい。また現フレームから変更するまでのフレーム数で示し、送信するフレーム毎にカウントダウンする方法でもよい。一般には、これらの信号の授受の際に信号受信に失敗する場合があります、それに対処するための確認のとりかたとして、確認信号が一定時間内に来ない場合に再送する方法や、確認信号が来るまでは指定信号を無条件に連続送信する方法等がある。

【0013】最初に示した変更タイミングまでに信号授受が成功しそうでないことを検出した場合には、指定動作の途中に変更タイミングを変更すればよい。演算鍵を変更した後、変更タイミングに不一致があれば、制御チャネル情報の授受もできなくなるので、フレーム同期用信号が受信できても制御チャネル情報や通信チャネル情報の授受ができない場合には、一定時間経過後、元の演算鍵に戻して、再度変更タイミングの指定を行う等の動作により、変更の確実性を増すことができる。

【0014】演算処理が、演算鍵と時刻(超フレーム開始タイミングからの経過フレーム数)の入力だけで定まる場合は、前記実施例を容易に実施できるが、演算処理が前フレームの演算結果を次フレームの処理に用いる等の逐次処理をしている場合、即ち、前記2入力だけで即時に演算できない処理の場合は、変更タイミングを確認しあってから実際の変更までの間に、変更前の鍵による通信を継続しながら変更後の演算処理の準備をすることによりこの発明の実施可能となる。

【0015】なおこの発明は移動通信における前記移動局番号による通信から加入者番号による通信への変更に適用する場合に限らず、一般に通信中に鍵変更のように演算方法を変更する場合に適用できる。また超フレームとしては演算処理により、最初の状態に戻らない無限大周期となる場合もある。しかしその超周期上の時間的位置、前記例では超フレーム内のフレーム位置は、送信側及び受信側で同期しているようにされる。

【0016】

【発明の効果】以上述べたようにこの発明によれば、変更タイミングを超周期内の時間的位置の情報として送信し、これを通信相手が受信したことを確認して変更タイミングで演算方法を変更するため通信が中断することなく通信中に暗号化等の演算処理を変更することができ、しかもその確実性も高い。

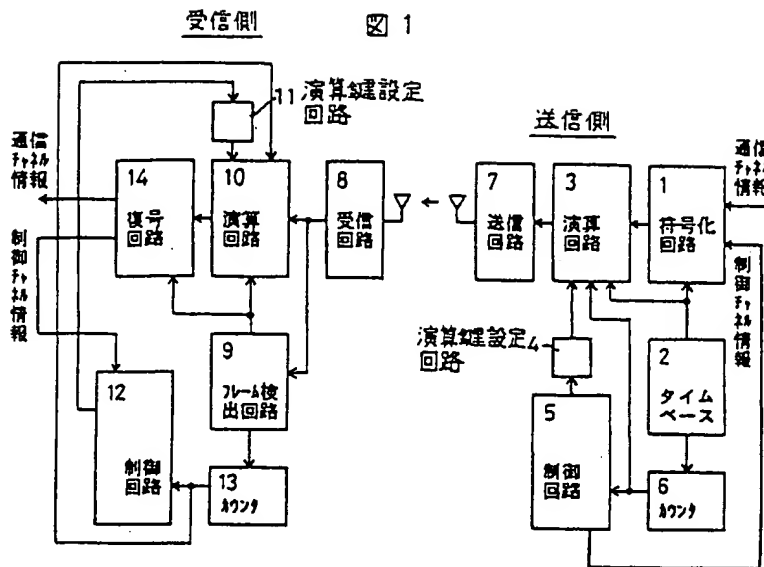
【図面の簡単な説明】

【図1】この発明の実施例を実行する通信ノードの構成を示すブロック図。

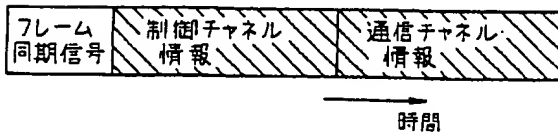
【図2】信号のフレーム構成例を示す図。

【図3】この発明の実施例における演算鍵の変更手順を示す図。

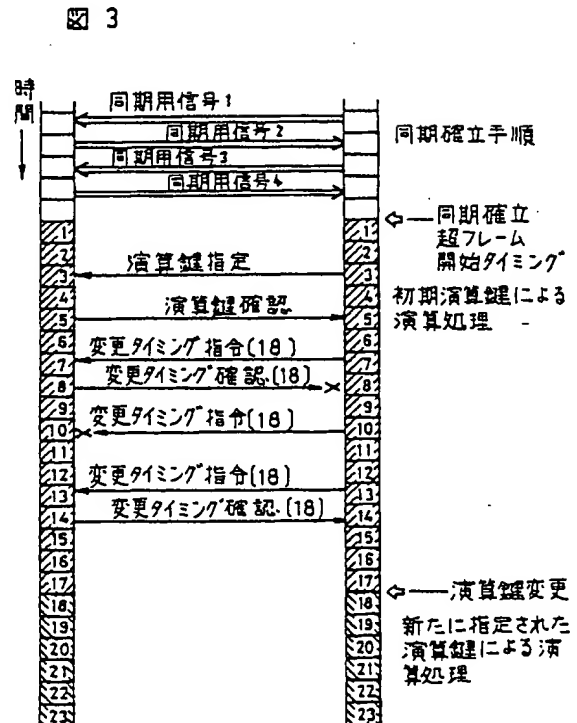
【図1】



【図2】



【図3】



フロントページの続き

(72)発明者 今栄 清志

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

This Page Blank (uspto)